

REASONS FOR ALLOWANCE

1. The following is an examiner's statement of reasons for allowance:

The prior art of record does not teach for fairly suggest the a multiple modulus selector having a modulus recoder for generating a first selection signal, a modulus selector for generating a second selection signal, and a multiplexer for receiving inputs $-M$, 0 , M , and $2M$ and selecting one of the inputs based on the first selection signal in an integer modular multiplication mode and selecting one of the inputs based on the second selection signal in a polynomial modular multiplication mode as recited in claim 2; or a multiple modulus selector for selecting one of $-M$, 0 , M , and $2M$ as a multiple modulus in an integer modular multiplication mode and selecting one of 0 , M , and $2M$ as a multiple modulus in a polynomial modular multiplication mode to output a multiple modulus accumulation indicating signal as recited in claim 12; or a booth recoder having a first selector for generating a first selection signal, a second selector for generating a second selection signal, and a multiplexer for receiving first inputs $-M$, 0 , M , and $2M$ and selecting one of the first inputs based on the first selection signal in an integer modular multiplication mode and receiving second inputs 0 , A , and $2A$ and selecting one of the second inputs based on the second selection signal in a polynomial modular multiplication mode as recited in claim 17

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chuong D. Ngo whose telephone number is (571) 272-3731. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lewis, Jr. A. Bullock can be reached on (571) 272-3759. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Chuong D Ngo/
Primary Examiner, Art Unit 2193

01/20/2009